AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS

1-2. (Cancelled)

3. (Currently Amended) An intelligent identification card comprising:

an on-board memory for storing reference data;

an on-board sensor for capturing live biometric data;

an on-board microprocessor for comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold; and

an interface for communicating the verification message to an external network,

~~wherein the verification message includes at least excerpts from the stored reference data, and~~

wherein the verification message includes at least excerpts from the captured biometric data, the verification message being transmitted to a remote authentication system for additional verification using reference data which is different from the reference data stored on said on-board memory.

4-5. (Canceled)

6. (Currently Amended) The identification card of claim 3 ~~claim 4~~ wherein the on-board microprocessor uses a different matching algorithm than that used at the remote authentication system.

7-8. (Cancelled)

9. (Previously Presented) The identification card of claim 3 wherein the card is ISO SmartCard compatible.

10. (Previously Presented) The identification card of claim 9, wherein said on-board processor is a security processor for storing and processing the protected biometric data, and wherein said identification card further comprises an ISO SmartCard processor.

11. (Previously Presented) The identification card of claim 10 wherein the security processor is functionally separated from the ISO SmartCard processor by a firewall.

12. (Previously Presented) The identification card of claim 10 wherein all external data to and from the security processor passes through the ISO SmartCard processor.

13. (Previously Presented) The identification card of claim 10 wherein all external data to and from the ISO SmartCard processor passes through the security processor.

14. (Previously Presented) The identification card of claim 10 wherein the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network.

15. (Previously Presented) The identification card of claim 14 wherein the first connection is permanently disabled after the loading process has been completed.

16. (Cancelled)

17. (Previously Presented) The identification card of claim 10 wherein:

the card comprises an upper magnetic stripe region and a lower embossed region;

the biometric sensor is a fingerprint sensor; and

the security processor, the ISO SmartCard processor and the fingerprint sensor are all located in a middle region between the upper region and the lower region.

18. (Previously Presented) The identification card of claim 3 wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor.

19. (Previously Presented) The identification card of claim 18, further comprising:

an indicator providing real-time feedback for finger placement while the user is manipulating his or her finger over the fingerprint sensor, thereby facilitating an adequate placement of the finger over the sensor.

20. (Previously Presented) The identification card of claim 18 wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data.

21. (Previously Presented) The identification card of claim 18 wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate.

22. (Previously Presented) The identification card of claim 21 wherein the backing plate comprises a glass epoxy layer sandwiched between two metal layers.

23. (Previously Presented) The identification card of claim 21 wherein the backing plate is reinforced by a carrier frame surrounding the sheet of silicon.

24. (Previously Presented) The identification card of claim 3 wherein the card further comprises means for restricting use of the card to a predetermined location.

25. (Previously Presented) The identification card of claim 3 wherein at least some of the captured biometric data and the reference data are transmitted to a separate authentication server for secure verification of a user's identity prior to any grant of on-line access to an application server for processing of secure financial transactions involving that user.

26. (Previously Presented) The identification card of claim 3, wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid.

27. (Previously Presented) The identification card of claim 3 wherein the output from the card is used to obtain physical access into a secure area.

28. (Previously Presented) The identification card of claim 27 wherein a record of successful and unsuccessful access attempts is maintained on the card.

29. (Previously Presented) The identification card of claim 3 wherein said interface includes at least one of:

an electrical contact interface; and

a wireless communication interface.

30. (Currently Amended) An intelligent identification card comprising:

an on-board sensor for capturing live biometric data;

a first on-board processor coupled with said on-board sensor, said first on-board processor including a memory storing reference data, said first on-board processor comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and generating a verification message only if there is a match within a predetermined threshold;

a second on-board processor coupled with said first on-board processor, for executing intelligent card functions, the verification message enabling said second on-board processor; and

an interface coupled to either one of said first on-board processor and said second on-board processor, for communicating with an external network~~, the verification message being transmitted to the external network via said interface~~.

31. (Previously Presented) The identification card of claim 30, wherein said second on-board processor is an ISO SmartCard processor.

32. (Previously Presented)The identification card of claim 31, wherein the first on-board processor is functionally separated from the ISO SmartCard processor by a firewall.

33. (Previously Presented) The identification card of claim 31, wherein all external data to and from the first on-board processor passes through the ISO SmartCard processor.

34. (Previously Presented) The identification card of claim 31, wherein all external data to and from the ISO SmartCard processor passes through the first on-board processor.

35. (Previously Presented) The identification card of claim 34, wherein the first on-board processor has a first connection used for loading data during a loading process and a second connection connected to an external network.

36. (Previously Presented) The identification card of claim 30, further comprising:

an on-board location detector for determining current location of the identification card; and

means for restricting use of the card based on the detected location.

37. (Previously Presented) The identification card of claim 36, wherein said on-board location detector includes:

a Global Positioning Satellite (GPS) signal receiver.

38. (Currently Amended) The ~~An~~ intelligent identification card of claim 30, further comprising:

~~an on-board memory for storing reference data;~~

~~an on-board fingerprint sensor for capturing fingerprint data;~~

an indicator for providing real-time feedback for finger placement while the user is manipulating his or her finger over the fingerprint sensor, thereby facilitating an adequate placement of the finger over the sensor~~;~~

~~an on-board microprocessor for comparing the captured fingerprint data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold; and~~

~~an interface for communicating the verification message to an external network~~.

39. (Currently Amended) A method for identifying a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data and an on-board biometric sensor, said method comprising:

capturing live biometric data using the on-board sensor;

comparing the captured biometric data with corresponding reference data stored in the on-board memory within a predetermined threshold;

generating a verification message only if there is a match within the predetermined threshold; and

communicating the verification message to an external network, the verification massage including at least excerpts from the captured biometric data;

~~wherein the verification message includes at least excerpts from the stored reference data, and~~

~~wherein the verification message includes at least excerpts from the captured biometric data~~

additionally verifying the user at a remote authentication system using reference data which is different from the reference data stored on said on-board memory.

40-41. (Canceled)

42. (Currently Amended) The method of claim 39 ~~claim 40~~, wherein a matching algorithm used in the identification card is different from a matching algorithm used at the remote authentication system.

43. (Previously Presented) The method of claim 39, further comprising:

transmitting at least some of the captured biometric data and the reference data to a separate authentication server for secure verification of a user's identity prior to any grant of on-line access to an application server for processing of secure financial transactions involving that user.

44. (Previously Presented) The method of claim 39, further comprising:

receiving a match request relating to a particular logon attempt at a particular application server; and

executing, if a positive match is produced at an authentication server in response to the match request, a secure three-way authentication protocol, the authentication protocol including:

sending a challenge character sequence from the authentication sever to the identification card;

generating, at the identification card, a challenge response based on the challenge character sequence and the match request;

forwarding the challenge response to the application server;

forwarding the challenge response from the application server to the authentication server; and

verifying, at the authentication server, whether the challenge response is valid.

45. (Previously Presented) A method for identifying a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data, an on-board biometric sensor, a security processor, and an ISO card processor, said method comprising:

capturing live biometric data using the on-board sensor;

comparing, using the security processor, the captured biometric data with corresponding reference data stored in the on-board memory within a predetermined threshold;

generating, using the security processor, a verification message only if there is a match within the predetermined threshold, the verification message enabling the ISO card processor;

~~communicating the verification message to an external network via an interface~~; and

allowing operation of the ISO card processor if the identity of the user is verified.

46. (Previously Presented) The method of claim 45, further comprising:

loading data onto the security processor via a first connection during a loading process; and

permanently disabling the first connection after the loading process has been completed.

47. (Previously Presented) The method of claim 45, wherein all external data to and from the ISO card processor passes through a second connection of the security processor.

48. (Previously Presented) The method of claim 45, wherein all external data to and from the security processor passes through the ISO card processor.

49. (Previously Presented) The method of claim 45, wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor.

50. (Previously Presented) The method of claim 49, further comprising:

providing real-time feedback for finger placement while the user is manipulating his or her finger over the fingerprint sensor, thereby facilitating an adequate placement of the finger over the sensor.

51. (Previously Presented) The method of claim 45, wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data.

52. (Currently Amended) The method of claim 45, further ~~A method for identifying identity of a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data and an on-board fingerprint sensor, said method~~ comprising:

providing real-time feedback for finger placement while the user is manipulating his or her finger over the fingerprint sensor, thereby facilitating an adequate placement of the finger over the sensor;

~~capturing live fingerprint data using the on-board fingerprint sensor;~~

~~comparing the captured fingerprint data with corresponding reference data stored in the on-board memory within a predetermined threshold;~~

~~generating a verification message only if there is a match within the predetermined threshold; and~~

~~communicating the verification message to an external network~~.

53. (Currently Amended) An apparatus for identifying a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data and an on-board biometric sensor, said apparatus comprising:

means for capturing live biometric data using the on-board sensor;

means for comparing the captured biometric data with corresponding reference data stored in the on-board memory within a predetermined threshold;

means for generating a verification message only if there is a match within the predetermined threshold; and

means for communicating the verification message to an external network,

~~wherein the verification message includes at least excerpts from the stored reference data, and~~

wherein the verification message includes at least excerpts from the captured biometric data, the verification message being transmitted to a remote authentication system for additional verification using remotely stored reference data which is different from the local reference data stored on said on-board memory.

54. (Currently Amended) An apparatus for identifying a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data, an on-board biometric sensor, a security processor, and an ISO card processor, said apparatus comprising:

means for capturing live biometric data using the on-board sensor;

means for comparing, using the security processor, the captured biometric data with corresponding reference data stored in the on-board memory within a predetermined threshold;

means for generating, using the security processor, a verification message only if there is a match within the predetermined threshold, the verification message enabling the ISO card processor;

~~means for communicating the verification message to an external network via an interface~~; and

means for allowing operation of the ISO card processor if the identity of the user is verified.

55. (Currently Amended) The ~~An~~ apparatus of claim 54, further ~~for identifying identity of a user of an intelligent identification card, the intelligent identification card including an on-board memory storing reference data and an on-board fingerprint sensor, said apparatus~~ comprising:

means for providing real-time feedback for finger placement while the user is manipulating his or her finger over the fingerprint sensor, thereby facilitating an adequate placement of the finger over the sensor~~;~~

~~means for capturing live fingerprint data using the on-board fingerprint sensor;~~

~~means for comparing the captured fingerprint data with corresponding reference data stored in the on-board memory within a predetermined threshold;~~

~~means for generating a verification message only if there is a match within the predetermined threshold; and~~

~~means for communicating the verification message to an external network~~.

56. (New) The identification card of claim 30, wherein said interface includes at least one of:

a wireless interface coupled to said second on-board processor; and

a wired electrical interface coupled to said second on-board processor.

57. (New) The identification card of claim 56, wherein said wireless interface is an ISO compatible antenna providing both data and power transmissions.

58. (New) The identification card of claim 56, wherein said interface further includes:

a security antenna coupled to said first on-board processor via a power circuit, said security antenna only providing power to said first on-board processor.

59. (New) The identification card of claim 58, wherein said security antenna also provides power to said on-board sensor via the power circuit.

60. (New) The method of claim 45, wherein said communicating the verification message includes at least one of:

communicating via a wireless interface coupled to the ISO card processor; and

communicating via a wired electrical interface coupled to the ISO card processor.

61. (New) The method of claim 60, wherein said wireless interface is an ISO compatible antenna providing both data and power transmissions.

62. (New) The method of claim 60, further comprising:

providing power to the security processor via a security antenna and a power circuit coupled to the security processor, the security antenna and the power circuit being provided on the card.

63. (New) The method of claim 62, further comprising:

providing power to the on-board biometric sensor via the security antenna and the power circuit.